CRP-C0178-01

認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司

評価対象

申請受付日（受付番号）	平成20年2月21日 (IT認証8196)
認証番号	C0178
認証申請者	東芝テック株式会社
TOEの名称	日本語名: e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア 英語名: System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853
TOEのバージョン	V2.0
PP適合	なし
適合する保証パッケージ	EAL3
開発者	東芝テック株式会社
評価機関の名称	株式会社電子商取引安全技術研究所　評価センター

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成20年8月12日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「日本語名:e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア V2.0、英語名:System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 V2.0」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「日本語名:e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア V2.0、英語名:System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 V2.0」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である東芝テック株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：	日本語名:	e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア
	英語名:	System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853
バージョン：	V2.0	
開発者：	東芝テック株式会社	

1.2.2 製品概要

本製品は、東芝テック株式会社製のデジタル複写機「e-STUDIO520/600/720/850, e-STUDIO523/603/723/853」(以下「MFP」という。)に実装されるシステムソフトウェアである。システムソフトウェアは、MFPとして

の一般的な機能（以下「一般機能」という。）、及びHDDから削除されたユーザ文書データを完全に消去する機能を提供する。上書きにより完全に消去する機能は、一般機能処理後のHDD作業領域から削除されたユーザ文書データの消去、及びHDDの廃棄・交換時の削除されたユーザ文書データの消去であり、この機能により不正なデータの復元を防止する。

1.2.3 TOEの範囲と動作概要

TOEは、MFPを制御するシステムソフトウェアである。MFPの各部分との関係は、図1-2に示す。MFPは一般的なオフィス等に設置され、単独で複写機として利用される他に、図1-1 に示すようなネットワーク環境でも、FAX とのデータ送受信端末、メールサーバへのメール発信端末、リモートにあるPC のリモートプリンタとして使われる。
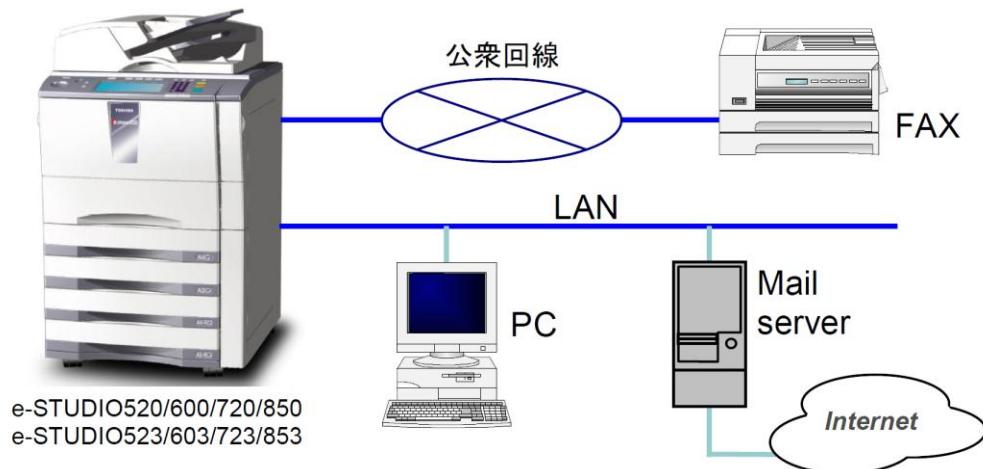
図1-1 TOEの利用環境例

MFPは、ユーザ文書を内部に取り込んで処理し出力する。MFPの出力に関係する処理には、コピー、プリント、スキャン、FAX 送信、FAX 受信の処理があり、各処理が完了したユーザ文書データは、MFP利用者がHDD の一時保存領域（下注）に保存する場合を除き、OS が提供するファイル削除機能で削除される。HDD の一時保存領域に保存されているユーザ文書データで不要になったデータは、MFP利用者が削除する。この場合も、OS が提供するファイル削除機能で削除される。しかし、OS が提供するファイル削除機能で削除した場合、OS が管理するファイル領域のポインタをクリアするだけであり、MFP利用者がHDD 内に存在していると思っていないユーザ文書データの実体が残留する。TOE は、ファイル削除されるユーザ文書データを完全に消去する機能と、HDD の廃棄・交換時に残留するユーザ文書データを一括して完全に消去する機能を提供する。

注記）本報告書では、ファイリングボックス及び共有フォルダを一時保存領域と

総称する。

1.2.4 TOEの機能

TOEは、利用者がMFPを使用するための通常モードとサービスエンジニアの保守のための自己診断モードを持つ。

1.2.4.1 通常モード

図1-2に通常モード時の構成を示す。
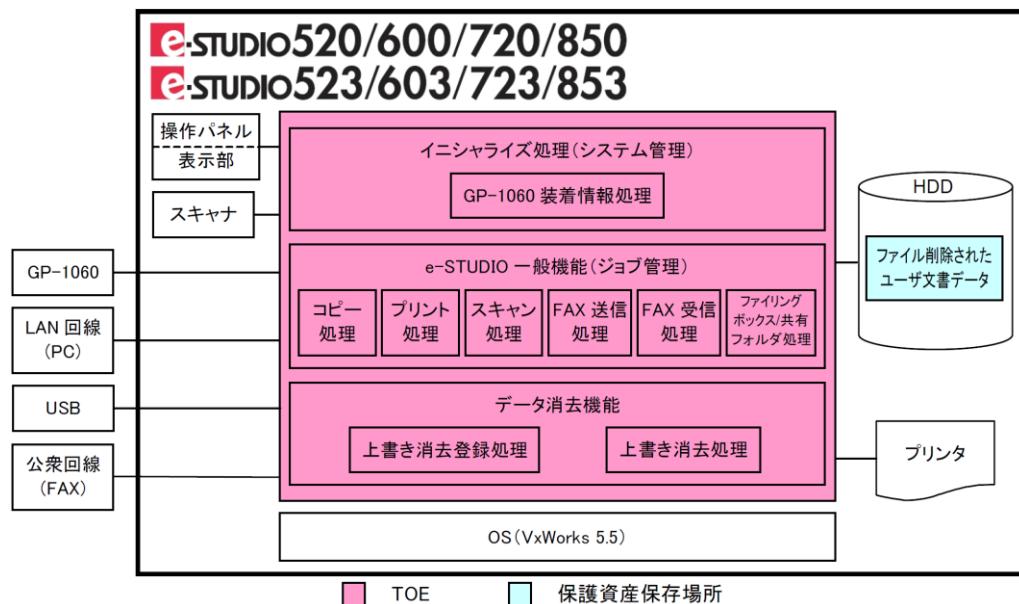
図1-2 通常モード時の構成

以下にTOEの処理内容を説明する。

1)GP-1060装着情報処理

GP-1060の装着を確認し、さらに、データ消去機能が有効になっていることを知らせるために、操作パネルにTOE名称とTOEバージョンを表示する。

2)コピー処理

スキャナからユーザ文書を読み取り、HDDの作業領域に書き出す。次に作業領域上のユーザ文書データを読み取り、プリンタへ出力、及び/または利用者が指定するHDDの一時保存領域に保存する。

3)プリント処理

ユーザ文書データをPCから受信、またはUSBから読み取り、HDDの作業領域に書き出す。次に作業領域上のユーザ文書データを読み取り、プリンタへ出力、及び/または利用者が指定するHDDの一時保存領域に保存する。

4)スキャナ処理

スキャナからユーザ文書データを読み取り、以下のいずれか、あるいは両方の処理を同時に行う。

- 利用者が指定したHDDのファイリングボックスまたは共有フォルダに保存する。あるいはWSスキャンにて指定したコンピュータへの送信を行う。
- 利用者が指定した送信先にE-Mail送信する。

5)FAX送信処理

スキャナからユーザ文書を読み取り、HDDの作業領域に書き出す。次に作業領域上のユーザ文書データを読み取り、FAX送信を行う。利用者が指定するHDD一時保存領域に保存することもできる。

6)FAX受信処理

FAXデータを受信し、HDDの作業領域に書き出す。次に作業領域のデータを読み取り、プリンタへ出力、及び/または利用者が指定するHDDの一時保存領域に保存する。

7)HDD一時保存領域の文書削除処理

操作パネル、またはPCの操作によってHDD一時保存領域上のユーザ文書データを削除する。

8)上書き消去登録処理(セキュリティ機能)

- 上記一般機能のそれぞれの処理において、HDD作業領域上のユーザ文書データの格納領域をダストボックスに登録する。
- 上記7)において、HDD保存領域のユーザ文書データ削除の削除操作が行われると、保存領域をダストボックスに登録する。

9)上書き消去処理(セキュリティ機能)

ダストボックスに登録されているユーザ文書データがあるか監視し、登録されている場合には、その領域を上書き消去する。なお、ユーザ文書データの消去処理中は、操作パネルにデータ消去中の表示を行う。MFP利用者は、印刷物の回収の際、操作パネルの表示によりデータ消去を確認する。

1.2.4.2 自己診断モード

図1-3に自己診断モード時の構成を示す。
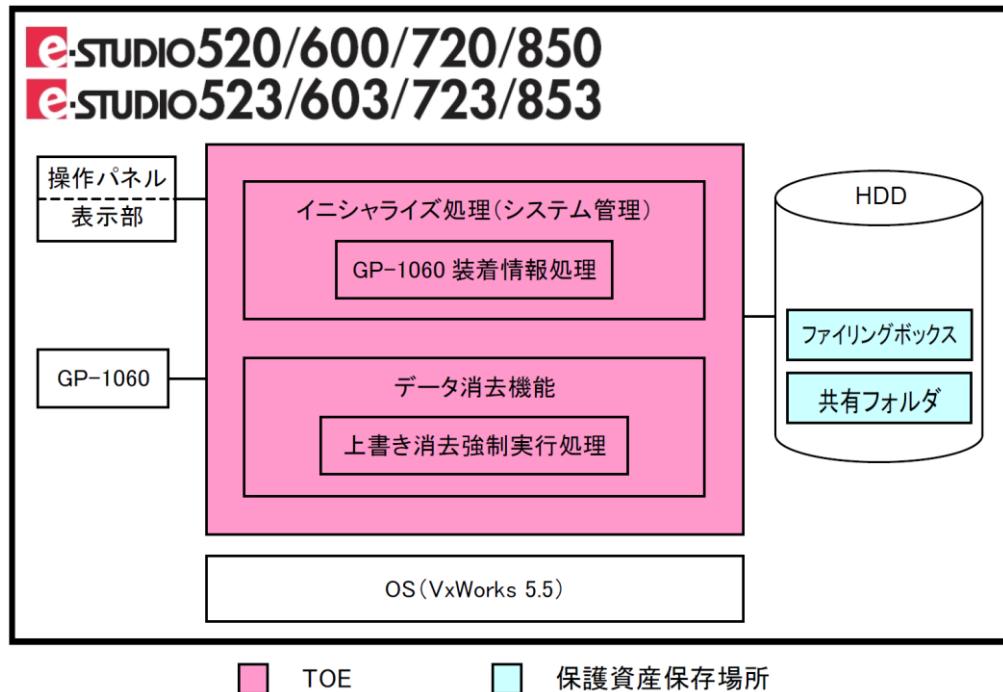
図1-3 自己診断モード時の構成

以下にTOE処理内容を説明する。

1) GP-1060装着情報処理

GP-1060の装着を確認し、さらに、データ消去機能が有効になっていることを知らせるために操作パネルに、TOE名称とTOEバージョンを表示する。

2) 上書き消去強制実行処理(セキュリティ機能)

HDDの廃棄・交換が生じ、HDDの一時保存領域に保存されているユーザ文書データを一括に削除する場合、HDDの全領域に対して上書き消去する。なお、消去は、サービスエンジニアが、MFP管理者からの依頼によって消去操作を行う。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。

② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

③　本TOEがセキュリティ設計に基づいて開発されていること。

④　上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 用 システムソフトウェアSecurity Target」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEの開発・製造・出荷の現場の過去の調査結果を確認し、本TOEがCCパート1（[5][8][11]のいずれか）附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア V2.0、System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 V2.0 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4　評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年7月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5　報告概要

1.5.1　PP適合

適合するPPはない。

1.5.2　EAL

STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3　セキュリティ機能強度

本STは、最小機能強度として、“SOF-基本”を主張する。

TOEは、一般的なオフィス環境に置かれ、想定する攻撃者の攻撃レベルは低レベルである。従って、最小機能強度として“SOF-基本”を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

SF.TEMPDATA_OVERWRITE

- 通常モードにおいて、HDD からファイル削除されるユーザ文書データの格納領域をダストボックスへ登録する。
- ダストボックスに登録されたHDD のユーザ文書データの格納領域に対して上書き消去を行う。 消去は、米国国防総省方式（DoD5220.22-M）に従って行う。(0x00Fill + 0xFF Fill + 乱数Fill + 検証)

SF.STOREDATA_OVERWRITE

- 自己診断モードにおいて、HDD の全領域に対して上書き消去を行う。消去は、米国国防総省方式（DoD5220.22-M）に従って行う。(0x00Fill + 0xFF Fill + 乱数Fill + 検証)

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.TEMPDATA_ACCESS	悪意を持った利用者または非関係者が人目につかずにMFPからHDDを取り外し、既存のツールを使用して、e-STUDIOのHDDから削除されたユーザ文書データを復元・解読することにより、ユーザ文書を取り出すかもしれない。
T.STOREDATA_ACCESS	悪意を持った利用者または非関係者が、既存のツールを使用して、廃棄または交換したe-STUDIOのHDDからユーザ文書を取り出すかもしれない。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.5.7 構成条件

本TOEは、東芝テック株式会社のデジタル複写機に実装されるシステムソフトウェアである。TOEの動作が評価により検証された条件を以下に示す。

- e-STUDIO520/600/720/850、e-STUDIO523/603/723/853のいずれかに、GP-1060と共に実装される。

- プリンタドライバとしては e-STUDIO850 Series PrinterDriver バージョン4.4.63.0が使用される。
- ファクスドライバとしては e-STUDIO850 Series N/W-Fax Driver バージョン2.1.8が使用される。
- ブラウザとしてはInternetExplorer ver6.0 sp1 または Firefox ver2.0.0.14が使用される。
- メーラとしてはAL-MaiL32 Version1.13 または Thunderbird ver2.0.0.14が使用される。
- WIA Scan Driver 対応アプリケーションとしてはWindows FAX とスキャン バージョン 6.0が使用される。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件はない。

1.5.9 製品添付ドキュメント

本TOE(日本語版)に添付されるドキュメントを以下に示す。

- e-STUDIO600/720/850 クイックスタートガイド OMJ070096A0 01
- Data Overwrite Kit(6カ国表示のデータ消去キット取扱説明書) OMM050034C0 03
- 取扱説明書[共通編] OMJ040119F0 06
- 取扱説明書[設定／登録編] OMJ040121E0 05
- GD-1170 取扱説明書[ファクス編] OMJ050013C0 03
- 印刷ガイド OMJ050004F06 03
- ファイリングボックスガイド OMJ07010700 00
- TopAccess ガイド OMJ07010400 00
- ネットワーク管理ガイド OMJ050010C0 03
- ネットワークファクスガイド OMJ07010000 03
- スキャンガイド OMJ07011000 00

本TOE(英語版)に添付されるドキュメントを以下に示す。

- e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 Quick Start Guide OME070095A0 02
- Data Overwrite Kit(6カ国表示のデータ消去キット取扱説明書) OMM050034C0 03
- Operator's Manual for Basic Function [北米版] OME040117C0 07
- Operator's Manual for Basic Function [欧州版] OME040118G0 07
- Operator's Manual for Basic Function [アジア版] ME050093E0 05
- User Functions Guide OME040120E0 05
- GD-1170 Operator's Manual for Facsimile Function OME050083B0 02
- Printing Guide OME050003E0 05
- e-Filing Guide OME07010600 00
- TopAccess Guide OME07010300 00
- Network Administration Guide OEM050009B0 02
- Network Fax Guide OME070097000 00
- Scanning Guide OME07010900 00

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年2月に始まり、平成20年7月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。同一の保証レベルの他のTOEの評価において、平成17年10月、11月、及び平成18年1月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査が行われた。本TOEにおいても同一のプロセスが実施されていることが確認されたため、プロセスの施行状況については、平成17年10月、11月、及び平成18年1月の調査結果を使用した。また、平成20年5月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を表2-1に示す。

表2-1 開発者テスト構成

TOE	バージョン		
TOE V2.0	項目	日本語版	英語版
	ROM	T390SY0J329	T390SY0U329, T390SY0E329
	システムソフト	VTR58.900	同左
	UI データフレーム	V0310.000 0	同左
機器	**主な仕様**		
デジタル複写機(MFP)	e-STUDIO850		
MFP のオプション	GP-1060		
テスト用 PC	OptiPlex GX100(DELL), OPTIPLEX 350(DELL)		
メールサーバ	SuperMicro 社製 5013C-MT Model P4SCT+		
デバッグ用基板、シリアルケーブル	シリアルポートドライバが実装された基板:6LA70328000 PWB-F-SERIAL-IF-360、DSUB 9 ピンコネクタのクロスケーブル		
FAX	e-STUDIO350 スーパーG3 を搭載した MFP		
擬似交換機	EXCEL7000		
ソフトウェア	**主な仕様**		
WIA Scan Driver 対応アプリケーション	Windows FAX とスキャン バージョン 6.0 (Windows Vista に含まれる)		
メーラ	AL-MaiL32 Version1.13		
Web ブラウザ	Microsoft Internet Explorer Version 6.0 Service Pack 1		
プリンタドライバ	e-STUDIO850 Series PrinterDriver バージョン 4.4.63.0		
ファクスドライバ	e-STUDIO850 Series N/W-Fax Driver バージョン 2.1.8		

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者テストは、STにおいて識別されているTOE構成と同一のTOEテスト環境とみなせることが評価者により確認された。

b.テスト手法

テストには、以下の手法が使用された。

①操作パネルからの操作＋プログラム動作状態のモニタリング

操作パネル上のキー入力操作、表示内容の確認を行い、加えて製品内部のプリント基板に専用のハードウェアを付加し、RS232C(シリアル通信)ポートを形成し、これに端末を接続する。開発者のみが可能な構成であり、各種解析用機能が提供され、プログラムの動作状態がモニタリング可能である。ハードディスクへのファイル生成、ファイル移動・上書き動作が行われている事が確認できる。

②リモートPCからの操作＋プログラム動作状態のモニタリング

リモートPC上のWEBブラウザからの操作、あるいはFAX、E-mail受信等の結果を確認するもの。加えて製品内部のプリント基板に専用のハードウェアを付加し、RS232C(シリアル通信)ポートを形成し、これに端末を接続する。開発者のみが可能な構成であり、各種解析用機能が提供され、プログラムの動作状態がモニタリング可能である。ハードディスクへのファイル生成、ファイル移動・上書き動作が行われている事が確認できる。

c.実施テストの範囲

テストは開発者によって105項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同等の環境に、以下が加えられた。

- メーラとしてThunderbird 2.0.0.14
- WebブラウザとしてFirefox 2.0.0.14
- 侵入テストに使用するツールとしてNmap 4.65.0.0

2）評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されたとみなせることが評価者により確認された。

b.テスト手法

テストには、開発者テストと同じ方法がとられた。

c.実施テストの範囲

評価者が独自に考案したテストを6項目、開発者テストのサンプリングによるテストを25項目、計31項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストで実施しているテスト項目のシナリオは全て網羅する

② インタフェースの種類に対して、最低限一つ以上のテストをテスト項目に含める

侵入テストは、開発者が考慮していない明白な脆弱性が存在しないかの確認のため、4件の侵入テスト項目を設定した。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3　認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

①　当該所見報告書でなされた指摘内容が妥当であること。
②　当該所見報告書でなされた指摘内容が正しく反映されていること。
③　提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④　評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤　評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、

	その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**

ACM_CAP.3.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、過去の検査結果により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。

ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。

ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。

ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。

脆弱性評定	適切な評価が実施された
AVA_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

MFP (Multi Function Peripherals) : デジタル複合機	コピー、プリンタ、ファックス等の機能を1 台に集約した多機能周辺機器。
e-STUDIO	TOE が実装されているMFP。e-STUDIO520/600/720/850、e-STUDIO523/603/723/853を指す。
HDD	Hard Disk Drive
ユーザ文書データ	e-STUDIO 一般機能を利用して、e-STUDIO 利用者の文書をデジタル化したデータ。ただし、FAX 受信データは送信者のデータでありe-STUDIO 利用者のデータではないため、ユーザ文書データから除く。
ファイリングボックス、共有フォルダ	e-STUDIO 利用者が、ユーザ文書データを一時的に保存・参照できる領域。データの削除は利用者が行う。保存有効期限が過ぎると削除されるが、このデータは、保護資産の対象としない。

GP-1060　　e-STUDIO520/600/720/850、e-STUDIO523/603/723/853に装着して、システムソフトウェア内のセキュリティ機能であるデータ消去機能を有効にするための製品。

利用者　　e-STUDIO 一般機能を利用するユーザ。

管理者　　e-STUDIOの一般機能の各種設定（コピー設定、ネットワーク設定、ファクス設定など）を行う。また、HDD の上書き消去強制実行をサービスエンジニアに依頼して消去を行わせる。

サービスエンジニア　　e-STUDIOの運用において、設置（GP-1060 の設置作業を含む）やインストール等の保守業務を行う。

6 参照

[1] e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 用 システムソフトウェアSecurity Target Ver3.3（2008年7月22日）東芝テック株式会社 画像情報通信カンパニー

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001 （平成17年12月翻訳第1.0版）

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002 （平成17年12月翻訳第1.0版）

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003 （平成17年12月翻訳第1.0版）

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 （平成17年12月翻訳第1.0版）

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512 平成17年12月

[18] e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェアV2.0、System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 V2.0 評価報告書 第1.1版 2008年7月24日 株式会社電子商取引安全技術研究所 評価センター

サーベイランス報告書

発行日	: 2012-08-17
資料番号	: SRP-C0178-01

下記評価対象(以下「本TOE」という。）について、ITセキュリティ認証申請手続等に関する規程(CCM-02)8.1に基づき、サーベイランスが実施されたことを報告いたします。認証報告書と合わせて参照願います。

評価対象：

認証番号	C0178
認証申請者	東芝テック株式会社
TOEの名称	日本語名: e-STUDIO520/600/720/850, e-STUDIO523/603/723/853用システムソフトウェア 英語名: System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853
TOEのバージョン	V2.0
PP適合	なし
適合する保証パッケージ	EAL3
開発者	東芝テック株式会社
評価機関の名称	株式会社電子商取引安全技術研究所 評価センター

サーベイランス管理番号：JISEC-SV12-001

サーベイランス実施報告：

- サーベイランス結果

本サーベイランスに関し、評価機関により本TOEを安全に消費者が利用することが可能であることが確認されたため、本TOEに対する認証は維持されます。

- サーベイランス概要

本TOEに関して開発者より公開された以下の「お知らせ」の内容に関し、認証を維持することが適切かどうかを判断するために2012年4月から同年7月にかけてサーベイランスを実施しました。

http://www.toshibatec.co.jp/page.jsp?id=2330

「お知らせ」によると、公表された脆弱性を利用することで、Webベースの管理ユーティリティ「TopAccess」の管理者向けのページにパスワードなしでアクセス可能とされています。

サーベイランスの結果、管理者向けのページへのアクセスはセキュリティ機能に影響しないことが、評価機関の責任において当時の評価で検証済であることが示されました。

詳細を以下に示します。

「TopAccess」の管理者向けのページからは、MFPの時計の日時や、ユーザ文書データを保存する有効期限などを変更することができます。公表された脆弱性を利用して「TopAccess」の管理者向けのページにアクセスした場合に、MFPの時計の日時や、ユーザ文書データを保存する有効期限などを変更できるかどうかについては、当時の評価では未調査です。

本TOEには有効期限が過ぎると保存されているユーザ文書データを自動的に削除する機能がありますが、削除後の残存データが保護資産ではないことが明記されています。

「TopAccess」の管理者向けのページから使用できるそれ以外の機能に対しても、評価対象であるセキュリティ機能への影響がないことが、評価機関において当時の評価で検証されていることが報告されています。

以上